R

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

C.A:04-1199 (SLR)

SRI INTERNATIONAL, INC., a California Corporation

Plaintiff and Counterclaim Defendant,

v.

INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware Corporation,

Defendants and Counterclaim-Plaintiffs.

COPY

VIDEOTAPED DEPOSITION

OF

Y. FRANK JOU

At Raleigh, North Carolina
January 27, 2006 - 9:53 a.m.

Reported by:
Debra D. Bowden

THIS PAGE HAS BEEN REDACTED IN ITS ENTIRETY

at the top, and 61.

A. 60. Okay. I'm there.

Q. And you'll see the entry on 60 near the bottom that's 82296.

A. Um-hmm.

Q. Now, according to J2, the meeting in Santa Cruz took place August 26th to the 28th of 1996.

A. Um-hmm.

Q. Does that sound about right?

A. Yeah.

Q. Okay. And then you have notes here, and then if you look on 61 --

A. Um-hmm.

Q. -- you have notes that go on for several pages.

A. Um-hmm.

Q. And it looks like this is a talk.

A. Yeah, that was the talk that I prepared for this, I believe, for this presentation. Yeah.

Q. For the presentation in Santa Cruz?

A. Um-hmm.

Q. Did you have any slides associated with

this presentation, or did you just give a talk?

A. I did have slides, as I recall, but I don't have any record, because after I left MCNC I probably, you know, gave it back to them.

Q. Well, keep this in mind. I have some presentations, and maybe we can identify things as we go along.

A. Sure. Okay.

Q. Now if you go back to the first page of J3, your notebook.

A. Um-hmm.

Q. At the top it says 54. And --

A. Where?

Q. At the top. The number of the page.

MS. PRESCOTT: I believe it's the second page of the exhibits.

Q. I'm sorry. Second page with 54 at the top.

A. Um-hmm.

Q. And it says 12695. And then it has a figure. Is this the start of thinking about the JiNao project, or is this something else? And I should mention a third possibility, that the date is wrong.

A. Yeah, that's what I was thinking. Probably that was, you know, should be '96, rather than '95. Because you know, when you turn around a year -- that's a possibility, um-hmm.

Q. I do that all the time. So it looks like at least as early as January '96 is when you were starting to think about the JiNao project. Would that be accurate?

A. That's fair to say that, yeah, I think so.

Q. And if you go to the next page in the notebook, it's marked 55.

A. Um-hmm.

Q. The entry that's marked 2/12/96.

A. Um-hmm.

Q. Where you say components.

A. Um-hmm.

Q. And it talks about statistics -- stats based. Is that statistic based?

A. Correct, um-hmm.

Q. Protocol based; is that correct?

A. Correct, um-hmm.

Q. Is that what's called signature detection?

A. No, signature detection -- well, it could

be different meaning to different people. Signature detection -- I have to recall about it.

Yeah, I think you are right. One is called signature based. The other one is called anomaly based, if I recall. But the memory kind of vague right now, because this, too, if you just look at the term itself, you might get confused in the way that -- for instance basically the computing block of the detection module in the JiNao project, one was statistical based. The other one was protocol based. And I think, you know, protocol based, we use the term signature.

Basically the protocol have the certain logic to it, and it has certain, you know, signature behavior, if you will. Similarly, for the statistical-based analysis, is just similar to, you know, for instance now days people in the credit card business, they have a certain -- everyone have certain spending profile, if you will, right? And you know, you like to spend

certain amount of money, you know, each year in a certain category. That's how, you know, you can sort of identify. Month after month you can sort of view the profile of certain people's spending habit. And if it's deviate from that habit, then you can call an anomaly. So that was the notion of the statistical analysis. And the terms, you know, kind of same, kind of similar, but you know, we tried our best to differentiate this code differently. But I think the term was signature for the protocol analysis, and anomaly for the statistical base, yeah.

Q. Now in February of '96 --

A. Um-hmm.

Q. -- do you recall if these notes were before or after you submitted your proposal to the DARPA?

A. I don't -- do you have a BAA? When they announced the BAA?

Q. I do not.

A. You do not. Okay. That probably the better -- I don't recall, either. Yeah

yeah, it -- sorry, I couldn't --

Q. Maybe when we take a break I'll call to my office and see if we have that in house.

A. Yeah, that would tell us clearly, you know. Because we had reference date here, and if the BAA is before this, then certainly, you know, this is -- but I would think this must be the discussion notes I took, you know, between MCNC and NC State at the time to come up with the proposal. So definitely this would be after, I would say this is after the BAA is announced. But whether, you know, before we submit a proposal or not, I think that was the question I had. You know, whether this was before we submit a proposal or afterwards. Definitely, you know, the context of these notes was the discussion related to JiNao, and certainly that took place after we saw the BAA, as I recall.

Q. With respect to the stats based part of JiNao --

A. Um-hmm.

Q. -- did you use an algorithm that was

developed at SRI?

A. Yes, pretty much that was the phase algorithm. We might have modified certain parameters there, but the framework was borrowed from SRI, as I recall, called NIDES, N-I-D-E-S.

Q. And how did it come to be that you used the SRI NIDES algorithm?

A. Well, at that time, as I recall, DARPA actually promote the idea. You know, other people's -- you know -- the research results, you know. There is nothing preventing -- because we are not for commercial purpose. So actually that was encouraged by DARPA so that you can, you know, help others and come up with something more advanced. That was I think one of the reasons, you know, the project was selected, because we view it on top of them and come up with integrated solution.

Q. To your knowledge, was the NIDES algorithm used for network data, internet network data?

MS. PRESCOTT: Objection to form.

A. Network data? What do you mean by network data?

Q. Well, if you take a look on 55, you have some target protocols.

A. Correct. Um-hmm.

Q. And you say OSPF internet.

A. Um-hmm.

Q. Correct? And I assume that -- well, let me not assume. Let me ask. Were you looking to use those protocols as a data source for the JiNao project?

A. Data source for the JiNao project? Well, the JiNao originally, as I recall here, we were targeting several candidates. OSPF was one, PRNN was one, and another to be determined, although I recall here HTTP, high speed. Those are all the relevant internet protocols.

Well, ATM you can argue is not part of TCP/IP. But certainly at that time ATM was one of the competing force to be a prominent candidate to prevail in the internet arena at the time. So I think, all based on the candidate's protocols that

we were interested in protecting at that time, and OSPF finally was the target protocol that we chose to focus our effort upon.

Q. Did the NIDES algorithm -- well, let's step back. Did you receive a NIDES algorithm from SRI?

A. Did I receive? No. I basically searched the internet and -- basically we came up with this true complementary algorithm, if you will, one is statistical based, one is protocol analysis based. So you know, we look around how we implement this. And so we search around, and we understand NIDES already developed a certain very nice algorithm in the statistical analysis arena. So that's why we talked to SRI folks and, you know, get a -- a detail of their algorithm. And we use that as a base. Yeah.

Q. When did you start contact with SRI?

A. When did I start contact with SRI? I don't recall exactly, but somewhere around that time frame, I would say. After we

establish statistical algorithm as the component, one of the major component in our design, we did a prior search, if you will, and then we found out SRI has this algorithm available. Developed, I should say. And so we talked to them. As far as time frame, I don't recall, you know, exactly when that happened.

Q. Do you recall who you spoke with first at SRI about the statistical algorithm?

A. Did I recall who I spoke to first? I don't recall clear, exactly, but one of three persons, I would say, was Peter Neumann was one possibility, and Al was another one, and Phil Porras was another one. Yeah, I think one of three. I don't recall who I spoke to first, but yeah.

Q. And Al, you mean Al Valdes.

A. Yes.

Q. If you could page into the notes into the laboratory images 68 and 69. And you'll see the entry at 68 is 82796.

A. Um-hmm.

Q. And the top is Teresa Lunt. Do you see

that?
A. Yes, um-hmm.
Q. And the dates that J2 established for the Santa Cruz meeting was August 26th and 27th. Or August 26th to 28th. So August 27th would perhaps indicate that this was at the Santa Cruz intrusion detection meeting.
A. Um-hmm.
Q. Looking over these notes, do these appear -- do you recollect that these are your notes?
A. Yes.
Q. From that meeting?
A. Um-hmm.
Q. And at the top it says Teresa Lunt.
A. Um-hmm.
Q. Who is Teresa Lunt?
A. She was the project manager at DARPA at that time.
Q. And the first entry, it says reusable modules designed to standard agreed upon. What does that mean?
A. I think this is in the context of CIDF.

Basically at that time we tried to -- all the PI's come together, try to design a common framework for all the project able to, you know, work together. Type of, you know, to create a synergy, if you will, among the projects. And this is to basically, you know, we come up with certain interface among the project, you know. For instance the detect results from one project can be fit into the second project. And the extender, basically everybody have to agree, if I recall correctly. That's just my guess at this point.

Q. Now if you go down a little bit.

A. Um-hmm.

Q. Let's see, the sixth entry. It says N/W wide. Does that mean network wide --

A. Yes, um-hmm.

Q. -- view, rather than simply local views?

A. Um-hmm.

Q. Do you have a sense of what you meant there?

A. Basically that was the notion we subscribe

Yeah.

Q. I'm going to ask the court reporter to mark as J Exhibit 4 a document bearing production numbers ISS_00341800 to ISS_00342038.

(Exhibit J4 was marked.)

This document is entitled CMAD IV Computer Misuse and Anomaly Detection. And if you look at the bottom it says Monterey, California, November 12th through the 14th, 1996.

A. Um-hmm.

Q. Do you recall this conference? And I'll give you a little help. If you turn in two pages --

A. Um-hmm.

Q. -- it says Session 4 at the top.

A. Um-hmm.

Q. If you go down three entries --

A. Okay.

Q. -- there's an entry, Scalable Intrusion Detection for the Emerging Network Infrastructure, Y. Frank --

A. Um-hmm.

Q. -- Jou?
A. Yeah. I think I attended at that time. Yeah. Okay.
Q. And do you recall if somebody from SRI was also at the workshop?
A. I don't recall exactly. But I assume if they're named here, then they could have attended as well. Yeah.
Q. I have some more documents that might help, so let me mark those. I'm going to ask the court reporter to mark as J5 a document bearing production number SRIE 53920.

(Exhibit J5 was marked.)

And to mark as J6 a document bearing production number SRIE 53899.

(Exhibit J6 was marked.)

And to mark document -- I guess Exhibit J7 a document bearing production number SRIE 0053740.

(Exhibit J7 was marked.)

Now J5 through J7 are a series of e-mails.
A. Um-hmm.
Q. And going to the first one.

A. Um-hmm.
Q. You'll see it's an e-mail from Peter Neumann?
A. Um-hmm. Peter Neumann.
Q. Peter Neumann, sorry. Actually if you look at the bottom --
A. Um-hmm.
Q. -- entry it appears to be from you.
A. Yeah.
Q. To Peter Neumann.
A. Right.
Q. And Al Valdes. And it's dated October 21st, 1996.
A. Um-hmm.
Q. And it says, "Thanks, Peter, for your quick response. Yes, I'll be attending Monterey meeting."
A. Um-hmm.
Q. "Will it be possible for me to visit Al on 11/11, Monday, or 11/15?"
A. Um-hmm.
Q. Does this refresh your recollection as to whether you attended the Monterey meeting?
A. Yes, pretty much, yeah. It's -- yeah.

Q. Did you meet with Mr. Valdes about that time frame?
A. Yeah, based upon these, I think yeah, I did meet with him.
Q. Do you recall if you met with anybody else at SRI?
A. Do you mean during the conference, or afterwards, or --
Q. Afterwards.
A. Afterwards, if I recall correctly, I might have paid them a visit at SRI. And you know, to -- I visited them once. That's what I recall. But I don't know whether this was the time I visit them. But this might be that time. Yeah.
Q. Now, at your visit do you remember -- well, do you remember who you met with at SRI during that visit?
A. The main one I thought was Al. Because that was -- you know, Phil might be there as well, but I don't -- I couldn't be hundred percent sure, but if I visit them at that time, I think it's mainly to understand better what other statistical

methodology they developed, so basically went there to get a better understanding of the NIDES, the statistical module. Yeah.

Q. Do you remember what Mr. Valdes told you about the statistical methodology?

A. Well, basically they -- if I recall correctly, I got a technical report from them about this NIDES statistical algorithm. You know, so -- and basically he went over briefly with me, you know, how it came about, what's the gist of the algorithm. Yeah.

Q. Were there any discussions at this meeting about using network data as a data source for the statistical algorithm?

A. Network data? Are you referring to OSPF?

Q. Yes.

A. I thought, you know, we made it clear, our target, the target of our protection was neuro infrastructures, basically the OSPF. So I don't recall whether we made it clear again during that visit or during that conversation, but certainly that, you know, in our presentation we -- we made it clear

that we are trying to protect the OSPF network. Yeah. So actually it's not part of data. Okay, part of this is a bit of difference between the understanding, because when we talk about data we're talking about, you know, application data. We are not talking about, you know, if you look at a network package, right, network packet, then you have a, you know header. You have the payload. The payload is what we consider as data, and the header is the protocol enable, you know, the transmission of this -- the payload. So I just try to make sure, you know. That's why we talk about same thing here.

Q. Right. So if I use the term network protocol data, would that be clearer?

A. Well, just network protocol, I think that should be sufficient. Network protocol is referring to the stack, you know, of different -- for instance OSI, or ISO, it's kind of confused sometimes, seven layers. You know, you have different networks stacked. And that's related to how network

provide the contramechanism, allow finally -- you know, the target is to move the payload around, right, whether it's video or whether it's e-mail or whatever, and that's the pay load. We call data. That's probably what we refer to. And the target of this project is to protect the one particular area of the proctostat called the routing protocol, specifically called OSPF. That's the target we try to protect. Yeah.

Q. Thank you.

A. Sure.

Q. If we turn to J7, which is the third e-mail I gave you.

A. Yeah, um-hmm.

Q. This looks like it's imbedded e-mails, so it's dated -- the e-mail is dated Monday, November 4th, 1996.

A. Um-hmm.

Q. And it appears to be from Phil Porras to you.

A. Okay.

Q. And the bottom one that has the karats in

front of the words --
A. Um-hmm.
Q. That appears to be an e-mail that you had sent earlier?
A. Um-hmm.
Q. And in it you say we'll be attending our project kick-off meeting next week.
A. Um-hmm.
Q. Do you recognize this e-mail?
A. Yeah. I mean I think this is what I wrote, yeah. Um-hmm.
Q. And when you state you'll be attending our project kick-off meeting --
A. Um-hmm.
Q. -- do you recall what the -- what is meant by project kick-off meeting?
A. As I recall -- now when they decide to, you know, when your project was selected, there is a formal kick-off meeting so to get everybody agree upon, especially the contractor, subcontractor. And the contracting agent in that case I thought was Rome Lab, who oversee this project. So basically if I recall, the kick-off meeting

actually was held in the -- in Rome Lab, Massachusetts. And I don't recall when. Unless you have other e-mail to show, I don't recall when was that, you know, meeting took place.

Q. The e-mail back from Phil Porras to you was November 4th, 1996.

A. Um-hmm.

Q. Does that help you recollect whether the kick-off meeting was in the fall of 1996?

A. Yeah, should be that time frame. Yeah, should be that time frame.

Q. Now, you state in the second sentence, "In preparing this meeting we need to provide our contracting officer an estimate as to when our statistical module can be delivered."

A. Um-hmm.

Q. "Since our implementation will be based on yours --"

A. Um-hmm.

Q. "-- would you please give me a time frame when your revision will be ready?"

A. Um-hmm.

Q. Do you recollect what revision you were seeking from SRI?

A. At that time, based on these e-mail notes, probably they are under -- they underwent a revision of their algorithm. This is the best explanation I can come up with. And so they're perhaps fine tuning, perhaps, you know, some revision going on at that time. And they indicated that, you know, they will be able to provide with a revised version to us. So that was the question I posed on them, basically asking a feel, you know, because our project will be using theirs as a foundation of the base module. So I basically tried to interlock with them. You know, make sure our project will be able to deliver based upon their revised algorithm.

Q. Does this refresh your recollection as to -- well, let me rephrase that.

What did you mean by statistical module? Is that software?

A. That was a design in our architecture. One component is called statistical module.

All of the -- that's -- yeah, that's an architectural design. Interpretation, it was a software; correct.

Q. Did SRI give you software?

A. No. They have the algorithm developed, you know, and it was presented in the technical report form. And basically we used that algorithm as a base to implement, so the software was written by ourselves.

Q. Is this what you would call an architectural design document?

MS. PRESCOTT: Objection to form.

A. Which one?

Q. I'm trying to understand what they gave you.

A. They gave me the algorithm. Um-hmm.

Q. From the algorithm, could you then implement their statistical technique?

A. Yes.

Q. Ask the court reporter to mark at J8 document bearing production numbers ISS 00354559 to ISS 354606.

(Exhibit J8 was marked.)

This document is entitled Proceedings

of the Fourth Workshop on Future Directions in Computer Misuse and Anomaly Detection.

A. Um-hmm.

Q. And the page I'm interested in is page 17 of the document, which is ISS 354580.

A. Um-hmm. Okay.

Q. And if you take a look at it, it says Session 4: Intrusion Detection in the Large. Moderator and session editor, Gene Spafford.

A. Okay.

Q. And then it has a list of presenters.

A. Um-hmm.

Q. And your name is among that?

A. Where does that appear?

Q. Up here.

A. Oh, okay. Um-hmm.

Q. Did you provide a presentation at this session?

A. That's the same one, right?

Q. Right.

A. This Misuse CMAD IV?

Q. Yeah, in Monterey, California.

A. Yeah, I think so.

Q. In general do you recall the format of the session at this workshop?
A. The format? Just each, you know, presenter give about I would say 30 minutes -- I don't have the agenda here, but 20, 30 minutes of their material, and then, you know, any question, feedback. So this pretty standard seminar type, conference type of presentation.
Q. And when it says Session 4, did everybody at the workshop generally go to the session, or were there breakout sessions?
A. I don't recall correct -- exactly what's -- if you have an agenda somewhere I could probably tell you better, but -- okay. Here. Does it have time line? Doesn't have time line, huh?

Well, the best I can tell you is probably sequential. It's not breakout. It's session -- you know, Session 1, Session 2 in sequence. That would be the best way I would say.

Q. If we could go back to page 17 of Session 4.

Q. The second sentence says participate in the API meeting. Do you know what that is referring to?
A. API meeting. Okay. This is -- this was probably referring to CIDF discussion where API stands for application program interface. I think that's the -- basically talk about how different projects can integrate together based upon the standard agreed upon that we had talked about earlier. Yeah.
Q. So there was an industry group that was working on developing a standardized --
A. Well, that was CIDF. Stuart was the chair of the CIDF. You know, the common CIDF -- common intrusion detection framework, yeah. He was the one in charge of that. So that's how I based upon to -- expect to think, this was what he -- what I mentioned here about API discussion.
Q. And by Stuart, you mean Stuart Staniford?
A. Correct.
Q. Did you participate in CIDF?
A. Yes, I was.

Q. Did Phil Porras participate in CIDF?
A. I think he did as well. Yeah.
Q. Now, if you go to the second e-mail on this page.
A. Um-hmm.
Q. It indicates it's from Porras at csl.sri.com. Is that Phil Porras?
A. Yeah.
Q. And it was sent to you --
A. Um-hmm.
Q. -- April 1st, 1997.
A. Um-hmm.
Q. And it says, "Hi, Frank. We've been going forward with the design and initial implementation of our statistical analysis engine. It could be fairly beneficial to both our groups if --" I think that's supposed to be an if, not an of --
A. Um-hmm. Okay.
Q. "-- we discuss your system requirements and expected usage of the stats engine before the design and prototyping gets too far along on the process."
A. Um-hmm.

Q. "What do you think about coming out for a visit sometime, perhaps the week of the Oakland conference?"
A. Um-mm.
Q. Do you recall whether or not you went out to SRI in April, the spring of '97?
A. Well, as I said, I did pay them a visit, but I don't recall exactly a time. So early on we had a exhibition, talk about the visit there, right, so I don't recall exactly whether I paid them a visit this time, or in the prior, you know, e-mail exchange. I don't recall.
Q. And you testified earlier that you remember one visit?
A. Um-hmm.
Q. Is it possible that you could have visited SRI more than once?
A. There's a possibility of that as well. But definitely I visit them at least once. I should say that.
Q. At least once.
A. Yeah.
Q. Here he's asking you about your system

requirements and expected usage of the stats engine.

A. Um-hmm.

Q. Do you remember any discussion with Mr. Porras or anyone at SRI about your system requirements and expected usage of the stats engine?

A. Yes, I think the communication was, you know, we basically conveyed to them how we are going to use their statistical algorithm. And they basically help us to understand their technical report, and help us, based upon our understanding, we implement our own software.

Q. So they were going to help you implement the NIDES algorithm.

MS. PRESCOTT: Objection.

A. Correct.

Q. And if I remember correctly, you testified your target protocol was OSPF.

A. Yes. But bear in mind, though, you know, this OSPF -- two forwards. One is specifically, you know, we can protect it based upon the design. Secondly, the best

architecture design can be applied to OSPF or other type of protocol as well. So we just use OSPF as a prototype to demonstrate the capability. And, you know, there is no restriction from applying this to other protocol as well.

Q. Other types of protocol used to transmit information on the internet?

A. Yeah.

Q. And you said before, generally a network packet is made up of a header and a payload; correct?

A. Correct. Um-hmm.

Q. And so in the intrusion detection systems --

A. Um-hmm.

Q. -- the system would look at header information to help it detect potential intrusions?

MS. PRESCOTT: Objection to form.

Q. Is that correct?

A. Basically we would call sniffer. Okay? Basically we observe the network traffic, ongoing network traffic, and we pick up

certain -- for instance in this case OSPF protocol communication. And look at the -- you know, how protocol behave among different entities. Okay, how they transect -- they transect among the different device going out. And from there we extract the knowledge whether this product exchange is in the normal operation, or is it -- there is some anomaly attempts to, you know, damage a normal operation.

Q. Have the court reporter mark as Exhibit J14 a document bearing production number SRIE 0018819.

(Exhibit J14 was marked.)

And this is another e-mail regarding the Oakland conference, and it's from you. At least the header information indicates it's from you to Phillip Porras, April 9th, 1997. Do you see that?

A. Okay. Um-hmm.

Q. At the bottom you say, "Thanks, Phil. The schedule is fine with me. During my last visit I missed your NIDES demo. Do you

think it's possible to schedule one at this time?"

A. Okay, so I may have visited him twice, then, based upon this.

Q. Do you remember seeing a NIDES demo at SRI?

A. I don't recall. I don't recall, sorry. No.

Q. Ask the court reporter to mark as Exhibit J15 a document bearing production number SRIE 0052499. This is another e-mail.

(Exhibit J15 was marked.)

A. Um-hmm.

Q. And it appears to be from you to Mr. Porras; is that correct?

A. Um-hmm.

Q. And it's dated June 9th, 1997.

A. Um-hmm.

Q. And you state, "Thanks for the info of your new paper."

A. Um-hmm.

Q. Do you recollect what this paper might be?

A. No.

Q. Do you recall receiving, other than the NIDES statistical algorithm, do you

remember receiving anything else from SRI in terms of papers, presentations?

A. In general, I mean at that time, as I recall, EMERALD was ongoing as well, together with JiNao project. So I don't recall what this new paper was about, but you know, other than NIDES, certainly we were aware of the EMERALD project at that time as well.

Q. And did the stats algorithm that you received from SRI, was it NIDES, or was it also to be used for EMERALD?

MS. PRESCOTT: Objection.

A. That was based upon NIDES. From what I recall. Whether they used in the EMERALD I cannot say for sure at this point.

Q. Will the reporter please mark as Exhibit J16 a document bearing production number SRIE 399190.

(Exhibit J16 was marked.)

If you look at this e-mail, it's dated June 18th, 1997. And it states -- appears to be from you to Mr. Porras, Mr. Wu, and Mr. Staniford; is that correct?

A. Um-hmm.
Q. Is that Felix Wu?
A. Um-hmm.
Q. And is that Stuart Staniford?
A. Yes.
Q. And is that Phillip Porras?
A. Yes.
Q. And the title is "How is your API proposal effort coming?" You see that?
A. Yes. Um-hmm.
Q. In the second paragraph it says, "Felix is going to make a personal trip to visit his parents in Freemont, California --"
A. Um-hmm.
Q. "-- on 6/26. He will stay there until early August. He agreed to pick up this task with Phil while he was there."
A. Um-hmm.
Q. Were Mr. Wu and you and Phillip Porras working together on the API proposal for CIDF?
A. Yes, I think that was the -- yeah, I don't recall, but this certainly, yeah, remind me of that. Correct.

Q. Do you see in the second paragraph, "I downloaded his newer version of EMERALD's paper?"
A. Yeah. Um-hmm.
Q. Does this remind you that -- of the earlier reference --
A. Um-hmm.
Q. -- regarding the paper, that you may have downloaded an EMERALD paper?
A. Yeah, I would say high possibility that this is referring to the EMERALD.
Q. Do you have any recollection of what that paper might have -- whether it was a technical description, or a paper for a conference?
A. I don't recall.
Q. Ask the court reporter to mark as J17 a document bearing production number SRIE 0399295. And also to mark as J18 a document bearing production number ISS_00357064 to ISS_00357136.

(Exhibits J17 and J18 were marked.)

Now turning to J18, do you recognize this technical report?

A. Yeah. Um-hmm.
Q. Did you help write this report?
A. Yeah.
Q. And this was the technical report from JiNao; is that correct?
A. Um-hmm.
Q. Now, if we turn to J17.
A. Okay.
Q. Actually going back to J18.
A. Okay.

MS. PRESCOTT: Excuse me. I don't know if you realize, but there appears to be another document attached to the back of this.

Q. Yeah. That must have been produced all together. That's a slide presentation.

So looking at the first part of J18 up through ISS_00357105.

A. Okay.
Q. That's the technical report. As Ms. Prescott points out, there's a document attached which is the slide presentation, which we'll get to later.
A. Okay.

Q. So the technical report, it says it was submitted, on the cover page, April 1997.
A. Yeah.
Q. Do you know what that means?
A. What do you mean, what that mean? This will -- periodically I would say any of the -- if I recall correctly, we had to submit our progress report to DARPA. Yeah, I think this is one of the, you know, scheduled report that we deliver as part of the project reviews.
Q. Now, if you turn to J17, which is the e-mail.
A. Yeah.
Q. This is an e-mail that states it's from you.
A. Um-hmm.
Q. Dated April 25th, 1997.
A. Right.
Q. There is a list of people that you distributed the e-mail to, and the subject was technical report available.
A. Um-hmm.
Q. And you say, "Dear PI's, we have

completed --" and let me read it. It's easier just to read it -- "as the first deliverable under JiNao project (Scalable Intrusion Detection for the Emerging Network Infrastructure). We have completed the system architecture design. It is available for access from http://www.mcnc.org/HTML/ITD/ANR/JiNao.html.

Did you take J18, the technical report, and put it on the web?

A. I think so. Yeah.

Q. Was it publically available as of April 25th, 1997?

A. Looks like, yeah.

Q. Do you recall putting it on the internet site for MCNC?

A. Yes, based upon this e-mail, yeah.

Q. And based on the distribution list, you sent it to all the DARPA PI's for intrusion detection.

A. Yes, correct.

Q. And that includes Peter Neumann, and you can see the distribution list, the third one down.

A. Yeah.
Q. It also included Porras?
A. Correct.
Q. And it also included Mr. Valdes, which is --
A. Yeah. Um-hmm.
Q. Have you ever heard of the way back machine?
A. Way back machine?
Q. Um-hmm.
A. Doesn't ring any bell.
Q. It's an internet archiving organization.
A. Um-hmm.
Q. The next exhibits, I'm going to show you some material that we were able to take from this internet archiving web site.
A. Um-hmm.
Q. I think we're on J19. Will the court reporter mark as Exhibit J19 document bearing production number SYM_P_0527594 to -- that would be it. Hold on one second. I've got the wrong -- here we go. Too much paper.

(Exhibit J19 was marked.)

A. Kill a lot of trees.
Q. Now, if you take a look at this --
A. Um-hmm.
Q. -- this is, according to archive.org you can see at the bottom --
A. Um-hmm.
Q. -- it is supposed to be pulled off of the MCNC web site.
A. Um-hmm.
Q. And if you look in the middle, it has 1997, 10/17.
A. Um-hmm.
Q. According to their format, that represents October 17th, 1997.
A. Okay.
Q. And if you look above that and what looks to be from the web site, there's a date of June, 1997. You have the wrong one.

You know what, why don't we take a break. I think I need to organize the exhibits for a second. Why don't we take a break so I'll have a chance to organize it a little better?

VIDEOGRAPHER: This represents the

end of tape one in the deposition of Y. Frank Jou. Going off the record at 11:47.

(Continuing after lunch recess.)

VIDEOGRAPHER: Back on the record, this begins tape number 2 in the deposition of Y. Frank Joe. The videographer is Bob Collier for the firm of Capital Reporting of Raleigh, North Carolina. This deposition is being held at the offices of Smith Moore, Raleigh, North Carolina, on January 27th, 2006. The time is 12:34.

BY **MS. MOEHLMAN:**

Q. Good afternoon. I'm going to hand you several exhibits that have been premarked, and if you can build them up together, I think that's the easiest way to do this.

So the first exhibit is J20. It is bearing document production SYM_P_0527594. Deposition Exhibit J21 bears production numbers SYM_P_0527595 to 96. So if you can put it underneath and sort of build the stack .

MS. BROWN: What exhibit number did

you say this was?

Q. J21. Exhibit J22 bears document numbers SYM_P_0527597 to 601.

Exhibit J23 is an exhibit bearing document production numbers SYM_P_0527602 to 643.

A. Are these the same?

Q. Yeah, it's the same, but I'll explain. It's supposed to be bound together. That's why it's a little disorganized. So I'm going to try and build it back up.

So J24 is document bearing production number SYM_P_0527644 to SYM_P_0527709. Okay. All right, so before lunch I was trying to walk through this. And I think we can do it a little better now that we have the exhibits together. So if you look on the first page, you'll see that this is -- appears to be a web page. Do you recognize this?

A. Yeah, um-hmm.

Q. What is it?

A. This was posted on the MCNC web site. You know, present the active projects that are

ongoing on MCNC -- well, I should not say active projects, because I gather some of this, for instance Vistanet and Atilla, probably has concluded at that point in time. So this probably the project which, you know, either in the past or ongoing at that point. Yeah.

Q. Now, you see in the corner there, it says June 1997.

A. Yeah. Um-hmm.

Q. Does that indicate that this was the page that was up as of June '97?

A. It was -- I would say this was last updated at that time. That would be my best interpretation about that.

Q. And as we were discussing the part -- the bottom, URL is from this archive.org repertoire, and it indicates a date of picking this up off of the web of October 17th, 1997.

A. Um-hmm.

Q. Do you have any reason to doubt the accuracy that this was on the web at -- on October 17th, 1997?

A. No, I don't think so. Unh-uh.
Q. All right. So now if we turn to the next exhibit, which is J21.
A. Um-hmm.
Q. Now, when you press -- when you click on the web site of JiNao, the next one that came up would be J21, Scalable Intrusion Detection for the Emerging Network Infrastructure.
A. Okay.
Q. And is that -- is that in accord with your recollection of how the web site, the MCNC web site worked?
A. Yes.
Q. And again at the bottom, from the archive.org web site, it indicates that this was up on the web of October 17th, 1997. Would that be in accordance with your recollection?
A. Yes.
Q. Okay. Now, if you turn to the second page of J21, you'll see it says three related -- it says related information, and then it has three links you can click on.

A. Yeah, um-hmm.
Q. Okay. The first one of that is J22.
A. Okay.
Q. Okay. And this is -- this says PP presentation ANR MCNC.
A. Um-hmm.
Q. Okay. Do you recognize this document?
A. Yeah, I think so. Um-hmm.
Q. Okay. Start at the bottom. This indicates again that it was on the MCNC web site October 17th, 1997. Is that in accordance with your recollection?
A. Yeah.
Q. Do you have a sense of what this Power Point presentation is for? And I'll tell you, the one that's on the second page, SYM_P_0527098, is the Power Point presentation, and then the following is the H -- the text version.
A. Okay.
Q. So it's sort of two representations of the same thing, because the slide is very small.
A. Um-hmm.

Q. Do you recognize this slide at all?
A. Yeah, I think so.
Q. What is it?
A. That was the one-page highlight of this project. Basically the one on the left upper corner is the target environment. I suppose that's what this is.
Q. Um-hmm.
A. And the right-hand side, upper right-hand side is talking about new idea of this project. And the third quarter, left bottom corner, is talking about the impact, the conclusion of this project, what impact. Would this effort bear fruit. And the last quarter, the right-hand bottom one, is about the schedule of this project.
Q. Do you remember using this to provide a presentation to anybody?
A. Well, I don't recall. This was one-page summary type of thing. My -- I might have. You know. Just sort of one-page summary of what's been going on with this project, and where we are at this point in time in terms of the progress. Yeah, but certainly this

was on the web site, as I recall, you know, based on this documentation.

Q. Now the next exhibit, J23, is, as you rightly pointed out, a copy of the exhibit that we marked J18.

A. Um-hmm. Yeah.

Q. This is what came up, if you go back to the exhibit marked J21.

A. Okay.

Q. And you go to the second page of that.

A. Um-hmm.

Q. If you clicked on the link called architecture design report --

A. Okay.

Q. -- this is what came up.

A. Okay.

Q. Is that in accordance with your recollection?

A. Yeah. I think so, yeah.

Q. Okay. Now, if you go to the third link on the second page of Exhibit J21, you would get J24.

A. Okay.

Q. Which is the last one.

A. Um-hmm. Okay.
Q. Do you recognize J24?
A. Yeah, I think so.
Q. And this is a Power Point presentation; is that correct?
A. Um-hmm.
Q. It was co-written by you?
A. Yeah.
Q. And if it helps, as Ms. Prescott pointed out, at the end of Exhibit J18 there was a slide presentation.
A. Okay.
Q. It's right here. At the end of this. And that's a blown-up version of the slide presentation.
A. Okay.
Q. On J24.
A. Okay.
Q. You can use whatever one is easier for you to read.
A. That's fine.
Q. So going back to J24, at the bottom this again indicates that it was on the web as of October 17th, 1997. Is that in

accordance with your recollection?
A. I think so.
Q. And this presentation at the top, the first page of the presentation, says IDS program review.
A. Um-hmm.
Q. Do you know what IDS means?
A. Intrusion detection system.
Q. Do you recall if you presented this slide show anywhere?
A. Some form of it. You know, might be in the PI meeting, or in the conference paper presentation. Yeah. But I, you know, don't know exactly which conference or meeting I presented it in its entirety. What conference. But this was made available through the web site.
Q. So you believe that you presented it, or some form of it, at a conference.
A. Yeah. I would think so.
Q. And that this was also available on the MCNC web site.
A. That's correct.
Q. So we can put these aside. We're in the

home stretch.

A. Good.

Q. All right. Do you know what exhibit number I'm on?

Ask the court reporter to mark as Exhibit J25 a document bearing production numbers SRIE 0399156 to 0399159.

(Exhibit J25 was marked.)

And this is an e-mail, it says from Teresa Lunt dated July 20th, 1997. It says tentative agenda for the DARPA intrusion detection conference.

A. Um-hmm.

Q. If you look in the 'to' lines, do you recognize your name, second row?

A. Um-hmm.

Q. And Mr. Porras' name also in the second row?

A. Um-hmm.

Q. And Mr. Valdes' name, which is six lines down in the middle.

A. Okay.

Q. Do you remember an intrusion detection PI meeting in Menlo Park?

A. Well, yeah. I don't recall prior to this, but if you show me this then I have no reason to doubt that there was a PI meeting took place at that point in time. Yeah.

Q. So these intrusion detection PI meetings are taking place every quarter, is that --

A. No, every half a year.

Q. Every half year.

A. Right.

Q. And I believe you said that the principal investigators were expected to show up at these meetings.

A. That's correct. Um-hmm.

Q. If you take a look at the second page of this exhibit, you see project update.

A. Um-hmm.

Q. And then it has at 10:00 --

A. Right.

Q. -- your name.

A. Um-hmm.

Q. Do you recollect what you would have presented?

A. The progress report. You know, of this project at that point in time. Yeah.

between two modules.

A. Two systems.

Q. Two systems.

A. Um-hmm.

Q. And so why would he be interested in the type and format of the data that you would be feeding to the stats tool?

MS. PRESCOTT: Objection.

A. I don't recall when he mentioned that the test tool is either about the stats tool we did in JiNao or the stats tool he talk about in EMERALD. I don't recall exactly what he meant here. But from the high level, as far as I can recall, there's pretty much talking about interface between two systems. That's what I can, you know, get out of this exchange.

Q. And if I understood your earlier testimony, as part of the CIDF group, JiNao and EMERALD were a sub group that was looking to share data between the two systems; is that correct?

MS. PRESCOTT: Objection to the form.

A. Able to work together as a bigger system,

if you will. For detection of the potential of intrusion attempts.

Q. And is this the right, correct terminology? Would JiNao issue alerts? Would a JiNao monitor issue an alert?

MS. PRESCOTT: Objection to the form.

A. JiNao would monitor the network traffic, in particular routing -- OSP of routing protocol. In this particular implementation, product implementation, we were particularly looking for OSPF protocol exchange. And based upon the system we designed, implemented, we focus on the -- any anomaly or any signature, protocol signature that's proved to be harmful of this particular protocol. So JiNao was designed to monitor the routing protocol exchange, and to determine whether the network status at that point in time was normal or was under potential attack.

Q. And if it determined that it was under a potential attack --

A. Um-hmm.

Q. -- what would it output? What would the

JiNao monitor output?

A. Okay, if I recall correctly, that we have so-called normal management on top of this. And basically it would be reflected through the management chain.

Q. And would the cooperation between JiNao and EMERALD be that EMERALD would be able to take in that -- that report?

A. Well, that certainly was the attempt, you know. But I don't recall, you know, how far we went, you know. How far we accomplished at that time.

Q. And was it also the case that JiNao was trying to accept reports from EMERALD?

MS. PRESCOTT: Objection.

A. I would say yes. Again that was the attempt under CIDF, but I don't recall how much we did along that line.

Q. But you were trying to work together to achieve an interface between EMERALD and JiNao; correct?

A. Yeah, that was the -- you know, under the behest of our project program manager, Teresa Lunt. She asked us to look closely

at how we can work together. Yeah.

Q. And if I'm understanding the testimony today, there were a few ways that you were working together. One was sharing the -- the SRI folks providing the statistical algorithm to you; correct?

A. Right. NIDES.

Q. And the second way that we talked about was through the CIDF effort to create a common interface; correct?

A. Yes, that was the goal. Again, you know, as I recall -- actually I don't recall how, you know, how much -- how far we -- we accomplished along that goal, I should say.

Q. Okay. Was there any other ways in which you cooperated with the EMERALD folks at SRI?

A. Not further -- no. Not much after, you know, beyond the extent after this.

Q. Now, ask the court reporter to mark as J27 a document bearing production number SRIE 0018215.

(Exhibit J27 was marked.)

If you'd take a look at J27, this is

an e-mail from you to Phillip Porras dated September 18th, 1997.

A. Um-hmm.

Q. You talked about placing two files --

A. Um-hmm.

Q. -- at a particular web address.

A. Um-hmm.

Q. One is test bed.ps. And the other one is gated.log. Do you know what these were?

A. Test bed.ps is the post script form of the test bed configuration we had at that point.

Q. And the test bed would be --

A. JiNao test bed.

Q. Would that be --

A. That consists of, you know, several internet spots. Work station. And we reconfigure it to serve as a router, because it has multiple interfaces that would interface current installed there. And each one basically running GateD. GateD is the software which has the OSPF protocol imbedded. And the log, the second file, gated.log, basically was the -- the

one. Actually he intended to send some more exhibit, but you know, the hard copy, only these three pages ended over to me. And later on he did send me electronic copy of some of these, I suppose, but I didn't bring them with me.

Q. Did Mr. Blake send you any other e-mails besides an attachment to your subpoena?

A. Not as I recall, no.

Q. Did Mr. Blake tell you about why you needed to come here today?

A. Yes, he did explain that, you know, this was because I work on the JiNao project, and had something to do with patent dispute between, you know, three parties, and -- yeah.

Q. Okay. And so basically you came here today in response to the subpoena that ISS sent and Symantec issued to you; correct?

A. Yes.

MS. PRESCOTT: Let's just take a short break.

THE WITNESS: Okay.

VIDEOGRAPHER: Going off the record.

The time is 15:10.

(Continuing after recess.)

VIDEOGRAPHER: Back on the record, the time is 15:14.

MS. PRESCOTT: Thank you very much for your time today, Dr. Jou. I'm going to turn you back over to ISS's counsel.

MS. MOEHLMAN: And if we could switch places. Why don't we stay on?

Why don't we go off for a second.

VIDEOGRAPHER: Off the record. Time is 15:14.

VIDEOGRAPHER: Back on the record. The time is 15:16.

RE-EXAMINATION

BY MS. MOEHLMAN:

Q. Mr. Jou, I have a couple more questions, some follow-up questions that will be very short.

A. Okay.

Q. If you could take the technical report dated April 1997, J18.

A. Okay.

Q. If you could, turn to page 19 of that

report, which is ISS 00357089.

A. Page 21, right?

Q. Page 19.

A. 19.

Q. Let me try again. I'll give you the last one. 087.

A. Yeah.

Q. You're on the right page. And if you'll look on that page you'll see it says measures.

A. Um-hmm.

Q. Do you see that? And then if you read through the paragraph, about halfway down it talks about using the names of the packet types.

A. Um-hmm.

Q. And then there's a sentence that says, "We would classify the JiNao measures into two groups, activity intensity and audit record distribution measures."

A. Right, um-hmm.

Q. And then it goes on to talk about one of the measures for activity intensity measures being volume.

A. Um-hmm.
Q. Correct?
A. Um-hmm.
Q. Now, does that refresh your recollection of when you thought of using data volume as a measure?
A. Okay. May-April, '97. Okay. Yeah. Yes. And your question was what?
Q. Had you by April 1997 thought of using data volume as a measure in your JiNao system?
A. According to the -- this documentation, I would think so, yes. Um-hmm.
Q. And we established earlier in your testimony that this was posted on the web in April of 1997, this technical report; correct?
A. I don't recall when it was posted, but based upon the time stamp it was April, 1997.
Q. Just so the record's clear, if you could pull out J17.
A. J17.
Q. That's going to be an e-mail.
A. Can you just show me the one you have,

or --

Q. Well, it has my writing on it. Let me find it.

A. 17, here.

Q. Great. If you remember, J17 is an e-mail from you to a group of people dated April 25th, 1997.

A. Yeah.

Q. And you wrote that the system architecture design was available from the MCNC web site. Do you remember that?

A. Yeah.

Q. And that the system architecture design that was available is J18; correct?

A. Yeah.

Q. Okay. So as of April, the end of April, 1997, is it fair to say the Exhibit J18 was on the MCNC web site?

A. Okay, yeah. Um-hmm.

Q. So going back to J18, page 19, in that architecture document you talk about using data volume as a measure; correct?

A. Correct. Um-hmm.

Q. Now, going back to the J37 paper.

A. Okay.
Q. Keep J18 open to page 19.
A. Um-hmm. Okay.
Q. Now, go back to J37.
A. J37. Okay.
Q. Go to page 65 --
A. Okay.
Q. -- of that, which is SYM_P_0500580.
A. Yeah.
Q. Now, if you look, another of the measures that you talked about was in 4.2, OSPF type.
A. Yeah, right.
Q. Now, if you could put it side by side, this paper, with J18.
A. Okay.
Q. And at the end of the paragraph on measures, do you see where it says hello packets?
A. Um-hmm.
Q. And if you look at the paper from G -- J37, it lists number one, hello.
A. Um-hmm.
Q. Number two on the paper is data base